Recomendaciones a las empresas/personas en trabajo en casa – Ciberseguridad

Empresas

Activar la configuración multifactor en las cuentas de correo personales y corporativas, con el fin de confirmar la identidad del que accede al correo y demás herramientas.

Implemente en su organización y/o Entidad canales de comunicación seguros desde Internet como SSL VPN, para sus colaboradores y funcionarios en las conexiones para teletrabajo y trabajo remoto.

Si debe habilitar algún servicio de cara internet, primero evalúe el riesgo antes de realizar la actividad, que las acciones de contingencia no afecten la seguridad de los datos.

Mantenga actualizado su sistema operativo con los últimos parches de seguridad liberados por el fabricante.

Instale y mantenga actualizado el software antivirus, de un fabricante reconocido, para evitar infecciones con virus o software malicioso.

Tenga en cuenta las políticas de privacidad de la información, para no divulgar información sensible y privada de la organización o Entidad.

Implemente soluciones de almacenamiento como Onedrive y Drive coorporativo para guardar los archivos de los colaboradores a través de la infraestructura del servidor de archivos implementada.

Activar perfiles de navegación para los usuarios SSL/VPN permitidos.

Realice un monitoreo permanente a la infraestructura de los servicios utilizados por los teletrabajadores, con el fin de analizar posibles acciones no autorizadas.

Implemente validaciones de seguridad mínimas al momento de la conexión por SSL VPN, para dispositivos BYOD (Bring Your Own Device), como protección de antivirus, actualización de parches de seguridad entre otros.

Impedir guardar de forma automática las credenciales de usuarios asociadas a las herramientas corporativas.

Genere políticas de backup para evitar pérdidas de información.

Implemente políticas de cifrado en los equipos, servidores y herramientas transaccionales con el fin de mantener la protección de la información.

Implementar la segmentación (mínimo privilegio) en los recursos a los que se accederá de forma remota con el fin de garantizar que ante un acceso indebido al equipo que se está intentando conectar a la red, no pueda acceder a recursos y/o información que no es necesaria para ese usuario.

Hacer uso de herramientas de protección del dispositivo como EDR (Endpoint Detection and Response), los cuales permiten una gestión integral y centralizada de la política de seguridad de la empresa localmente en los dispositivos de los empleados.

Si los colaboradores hacen uso de dispositivos móviles para el ingreso a los servicios prestados por la organización y/o Entidad se debe prohibir el uso de dispositivos rooteados o a los que se ha realizado jailbreak.

Se debe asegurar que en caso de extravío de dispositivos se deben configuras medidas de seguridad para proteger la información corporativa (localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas).

Las empresas deben realizar un plan de formación y capacitación a sus empleados en el correcto uso de los medios tecnológicos.

Personas

Utilice doble o triple factor de autenticación al realizar transacciones financieras.

Cambie las claves el acceso a wifi y evite utilizar redes inalámbricas abiertas, puede presentarse pérdidas de información.

Realizar copias de seguridad de manera periódica haciendo uso de los medios de almacenamiento entregados por la organización y/o Entidad para tal fin.

No enviar archivos con información de la organización y/o entidad, por medios no oficiales como whatsapp, dropbox, wetransfer, correos de dominio gratuito, etc.

Cierre sesión cuando no esté usando el dispositivo, tanto en casa como en lugares públicos.

Mantenga actualizado su sistema operativo con los últimos parches de seguridad liberados por el fabricante, si trabaja desde su propio dispositivo.

Instale y mantenga actualizado el software antivirus, de un fabricante reconocido, para evitar infecciones con virus o software malicioso.

Tener un espacio adecuado para teletrabajar sin riesgo a perder información por causa de daño del equipo por la mala manipulación de alimentos, por ejemplo.

No instale programas o extensiones de navegadores de fuentes desconocidas ya que estas suelen traer malware el cual puede afectar sus dispositivos y extraer la información sensible.

Evite el uso de aplicaciones de escritorio remoto que no estén verificadas por la organización y/o entidad, estas herramientas pueden crear puertas traseras por medio de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y por lo tanto permitir el acceso a los equipos corporativos.

Optimice el uso del internet, dado que por un mismo canal se van a establecer todas las conexiones, priorice las actividades laborales en los horarios establecidos para que no sufra caídas del servicio.

Recuerde que, aunque se esté trabajando desde casa, siempre debe garantizar la seguridad de los datos y cumplir con las exigencias de seguridad impuestas por la organización y/o Entidad y la Ley de protección de datos personales.

Móviles

No enviar mensajes de texto con datos confidenciales, como información privada y detalles de tarjeta de crédito

Cifrar el dispositivo móvil, implementaremos en los dispositivos mecanismos de cifrado de la documentación además de los de autenticación de usuarios.

No conectar el celular a puertos USB desconocidos y no aceptar ninguna relación de confianza a través de USB sin asegurarnos de que la conexión es de confiable.

No conectarse a redes Wi-Fi públicas abiertas (o hotspots Wi-Fi)

No instalar ninguna aplicación que no provenga de una fuente de confianza, como las tiendas oficiales de Apps

No instalar aplicaciones que exijan permisos que pongan en riesgo la información confidencial (acceso a la agenda, geolocalización, etc.);

Realizar copias de seguridad periódicas sincronizadas con los servicios de nube.

Mantener actualizado el sistema operativo del celular.